# Acceptable Use Policy

**The Customer must, and must ensure that all Customer Entities, at all times comply with this Acceptable Use Policy when using the Products. Except as otherwise set out in this Acceptable Use Policy, defined terms will have the meanings given to them in the General Terms.**

The following terms and definitions apply to this Acceptable Use Policy:

- **"Sanctioned Person"** means any person that is: (a) named on any list of persons targeted by Sanctions maintained by a relevant competent authority; (b) owned or controlled, directly or indirectly, by any such person; or (c) organised under the laws of, or ordinarily resident, located, or incorporated in, a Sanctioned Territory.

- **"Sanctioned Territory"** means any country or territory that is, at the relevant time, itself the subject or target of comprehensive, country-wide or territory-wide Sanctions.

The Customer must notify Wireless Logic as soon as reasonably practicable of any violation of this Acceptable Use Policy and must cooperate in any efforts to stop or remedy the violation. Failure to comply with this policy may result in Products being suspended or terminated.

This policy is subject to change by Wireless Logic from time to time in accordance with clause 13.4 (Change to General Terms and Product Schedules) of the General Terms.

## 1 Use of the Services

1.1 The Customer is responsible for all use of the Products by Customer Entities and their employees, consultants, service providers and any person permitted by the Customer to access or use the Products.

1.2 The Customer must observe and comply (and must ensure that all Customer Entities comply) with:

(i) all Applicable Laws, instructions from Regulatory Authorities or law enforcement agencies (including for lawful intercept and cybersecurity purposes), and Codes of Practice (including obligations applicable if any related service offered by the Customer means that either Wireless Logic and/or a Customer is a provider of electronic communications, telecommunications, value added or related services);

(ii) any acceptable use policies and fair use policies of any Network Provider(s) who provides underlying connectivity services used by any Customer Entity, such policies as applicable at the relevant time being available upon the Customer's request to Wireless Logic from time to time;

(iii) any reasonable instructions (including specifications and training) notified to the Customer by Wireless Logic and/or the relevant Network Provider(s) from time to time for the use and/or marketing of the Products or which in Wireless Logic or any Network Provider's reasonable opinion prevent: (i) the transmission of illegal material; or (ii) the Systems from being impaired or damaged.

1.3 The Customer must:

(i) meet the relevant technical and security standards required for the receipt and any onward provision of the Products from time to time;

(ii) only market to and solicit Customer Entities in relation to its provision of Products using staff contracted to or employed directly by itself;

(iii) notify Wireless Logic reasonably in advance of any proposals for the provision of goods, services and/or software to Customer Entities which include Products and, where requested by Wireless Logic, identify Wireless Logic (and, as requested by Wireless Logic, the relevant Network Provider(s)) in proposals to Customer Entities which include Products; and

(iv) not act or omit to act in any way which will or may place Wireless Logic and/or the relevant Network Provider(s) in breach of any provisions of Applicable Law, a Code of Practice and/or any other licences or authorisations applicable to Wireless Logic and/or the relevant Network Provider(s), and co-operate fully with Wireless Logic to enable Wireless Logic and/or the relevant Network Provider(s) (as the case may be) to comply with all of the same.

## 2 Use Cases

2.1 Certain uses of the Products carry additional risk and are subject to the specific requirements set out in Annex 1 (Use Cases), in addition to (and without limiting) the rest of this Acceptable Use Policy.

2.2 Except as otherwise set out in Annex 1, defined terms will have the meanings given to them in the General Terms or elsewhere in this Acceptable Use Policy.

## 3 Unacceptable Use

3.1 The Customer shall not, and shall ensure that its Customer Entities shall not, throughout the Term and after termination of the Agreement, use the Products (or allow them to be used) in any way:

(i) that: (a) is illegal or unlawful in any relevant country (in such circumstances Wireless Logic may report the incidents to the police or any other relevant official organisation); (b) infringes the intellectual property rights of any person, including reverse engineering, disassembling or decompiling (or otherwise attempting to obtain the source code of) any software (including on a SIM); (c) is fraudulent; (d) disrupts the functioning of any network or system, including transferring data in unreasonable quantities or frequencies; (e) disrupts the access of any third party to any network or system; (f) transmits software viruses or other disabling or damaging programs; (g) is intended to gain, or attempt to gain, unauthorised access to any network or system; (h) intercepts a third party's communications; or (i) brings Wireless Logic or any Network Provider into disrepute;

(ii) to receive, transmit or store data which is: (a) offensive, obscene or indecent; (b) defamatory, threatening or discriminatory; (c) infringing the intellectual property rights or privacy rights of any person; (d) artificially inflated traffic; or (e) illegal or unlawful in any way;

(iii) which will or may injure or damage any persons or the property of any persons (whether or not employees, agents or representatives of Wireless Logic or any one or more Network Providers), the Systems or howsoever cause the quality of the Products to be impaired;

(iv) which will or may place Wireless Logic and/or the relevant Network Provider(s) in breach of any provisions of Applicable Law, a Code of Practice and/or any other licences or authorisations applicable to Wireless Logic and/or the relevant Network Provider(s) and the Customer shall, and shall ensure that its Customer Entities shall, co-operate fully with Wireless Logic to enable Wireless Logic and/or the relevant Network Provider(s) (as the case may be) to comply with all of the same; and

(v) which permits any third party (except to the extent permitted by Applicable Law) to copy, adapt, reverse engineer, decompile, disassemble, modify, adapt, or otherwise make derivative works to, or make error corrections to the Products in whole or in part.

3.2 The Products should not be used in any application that:

(i) is intended to cause death, personal injury, or physical damage to property;

(ii) presents a material risk to human life, critical infrastructure, or public safety; or

(iii) otherwise constitutes unlawful, harmful, or unethical use of connectivity services.

3.3 **Acceptable Usage Policy –** for certain Products, particularly those sold with "Unlimited" usage, Wireless Logic implements an acceptable usage policy. Inappropriate usage in breach of this acceptable usage policy (in addition to the above unacceptable use) would be considered as the following:

(i) Any usage outside normal commercial practice;

(ii) Any usage in devices which are not authorised by Wireless Logic;

(iii) Any usage made via automated means (also see Gateway section below); and

(iv) data usage where End Users regularly tether to 12 or more devices or have used more than the per connection per month threshold (detailed in the Tariff Addendum under inclusive usage) twice within a 6 month period.

3.4 Wireless Logic may investigate usage in order to ascertain whether a Customer's usage is in line with this Acceptable Use Policy and any acceptable usage policy where relevant under paragraph 3.2. If Wireless Logic reasonably suspects that Customer's usage is in breach of paragraph 3.1 or 3.2 and/or the acceptable usage policy where relevant under paragraph 3.3, Wireless Logic reserves the right, based on the severity of the misuse, to restrict Services, or to suspend or terminate the Services pursuant to clauses 22.1(f) (Suspension) and 23.4(d) (Termination) of the General Terms.

# 4 Fraudulent Traffic

4.1 The Customer shall not, and shall ensure that Customer Entities shall not throughout the Term use the Products for distributing fraudulent, deceptive, malicious, harmful, illegal or disruptive traffic ("**Fraudulent Traffic**").

4.2 Indicators that could be used as reference to determine Fraudulent Traffic may include but are not limited to the following:

(i) high share of traffic generated from a limited number of SIM-cards/A-Numbers/IMSIs;

(ii) high share of traffic to unusual service numbers (e.g. premium rate numbers, value added service numbers, conference service numbers, Satellite Networks, etc.) or to high cost third country other than to the HPMN network. Typically, it will be to a few B-numbers or B-Number ranges;

(iii) calls made with a high frequency;

(iv) calls with a long duration; and

(v) call attempts with a high frequency (generation of high signalling traffic).

# 5 Machine to Machine Services

5.1 The Customer shall ensure (and use all reasonable endeavours to ensure that Customer Entities ensure) that any Products supplied under the Agreement shall be used solely in relation to Machine to Machine Services and shall not use the Products to take any action that:

(a) involves the transmission of voice (including VOIP) unless expressly agreed otherwise (see section 7 below);

(b) involves providing any service via the Products that allows an End User or other person to access a publicly addressable destination (i.e. public IP address) including through the use of a proxy, tunnelling, a gateway or routing;

(c) would violate copyright, a trademark, a trade secret or other property rights of any third party;

(d) could interfere with other users' use of Wireless Logic's and/or the relevant Network Provider(s)' network;
(e) involves the addition, removal or modification of identifying network header information in an effort to deceive;
(f) uses the Products to access, or attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of Wireless Logic's and/or the relevant Network Provider(s)' or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data;
(g) uses the Products or software related to Internet relay chat ("**IRC**"), peer to peer file sharing ("**P2P**"), bit torrent, game servers or proxy server network;
(h) involves spamming or the sending of bulk unsolicited emails or commercial messages or maintaining an open SMTP relay; and/or
(i) could lead directly to death, personal injury, or severe physical injury or environmental damage (for example life support machines) due to the failure of the Product(s).

# 6 Equipment

6.1 The Customer must ensure that all equipment that is connected to the Network is compatible with the Network and suitable for Customer's intended purposes. Wireless Logic is not responsible for the installation and functioning of the Customer's equipment and/or End User equipment.

6.2 The Customer must not use any equipment that has not been approved for use in connection with the Products by Wireless Logic and the relevant Network Provider(s). If the Customer is not sure whether the Customer's equipment and/or End User equipment is so approved, it must notify Wireless Logic immediately.

6.3 The Customer must comply with any technical and security requirements and the reasonable instructions (including in relation to regulatory requirements) issued by any telecommunications services provider who provides underlying connectivity services used by the Customer. Wireless Logic reserves the right, at its sole and absolute discretion, to require the Customer to satisfy Wireless Logic that any equipment to be used in connection with the Products is fit for purpose and suitable and the Customer undertakes to Wireless Logic to comply with Wireless Logic's testing and other requirements in respect of the same.

# 7 Gateways

"**GSM Gateway**" means any equipment containing a SIM which enables the routing of calls from fixed apparatus to mobile equipment by establishing a mobile-to-mobile call.

7.1 The Customer shall not connect itself, nor allow any Customer Entity to connect, any GSM Gateways to the Systems: (i) where it is illegal to do so under applicable law (which may include the provision of electronic communication services to a third party); or (ii) where it is legal to do so under Applicable Law, without the prior written consent of Wireless Logic, which may be withheld at Wireless Logic's absolute discretion and which will be subject to compliance with Wireless Logic's policy on GSM Gateways as notified to the Customer from time to time.

7.2 The Customer shall cooperate with Wireless Logic at all times to ensure that any GSM Gateways that have been authorised by Wireless Logic and are connected to the Systems are and remain compliant with Applicable Law and Wireless Logic's policies.

7.3 If the Customer becomes aware that any of its End Users or third parties have established, installed or are using a GSM Gateway in an illegal manner, in breach of the Agreement or in breach of Wireless Logic's policies (as advised to the Customer from time to time), the

Customer shall notify Wireless Logic immediately and shall upon request from Wireless Logic provide to it all technical details of the GSM Gateway and its use.

7.4 The Customer shall comply with Wireless Logic's instructions to facilitate the disconnection of any GSM Gateway that breaches this section 7. Wireless Logic may require the Customer to repay to Wireless Logic any payments or bonuses paid to it in connection with GSM Gateways that are discontinued subject to this section 7.4.

7.5 Wireless Logic may alter or amend the contractual terms or commercial policy relating to GSM Gateways at Wireless Logic's discretion by giving no less than twenty (20) Business Days' prior notice.

# 8 VOIP

8.1 The Customer shall not use the SIMs or the SIM Services for Internet phone calls (Voice Over Internet Protocol (VOIP)) unless agreed in writing by Wireless Logic at its sole discretion. Any unagreed VOIP usage may result in the connection being terminated at Wireless Logic's discretion.

8.2 If Wireless Logic agrees to the use of VOIP, the Customer must comply with any relevant requirements of Applicable Laws and Regulatory Authorities (including in respect of emergency calling) and any other requirements notified to it in writing by Wireless Logic.

# Annex 1 – Use Cases

Where the Customer's, or any Customer Entity's or End User's, use of the Products falls within one of the use cases described below, the Customer must notify Wireless Logic in writing before that use commences (or, if already underway, as soon as reasonably practicable after becoming aware of it) and must comply with the obligations set out under the relevant heading.

## 1 Military and Defence Applications

1.1 The Customer must not, and must ensure that no Customer Entity or End User, uses the Products in connection with any Prohibited Use as set out in the Wireless Logic Group Statement on Prohibited Use: Military and Defence Applications reproduced in full below.

1.2 The Customer must notify Wireless Logic immediately if it becomes aware that the Products are being, or may be, used or are proposed to be used in connection with any military, defence, government security or dual-use application.

1.3 The Customer must provide Wireless Logic with such information as Wireless Logic reasonably requires to verify compliance with this paragraph 1 and the Statement below, and must cooperate in good faith with any such request.

**Wireless Logic Group Statement: Prohibited Use – Military and Defence Applications**

Wireless Logic group companies provide telecommunications connectivity airtime and data usage services to SIM Card(s) and certain hardware (i.e. routers) as ordered by our business customers ("Services").
The Services and technology provided by Wireless Logic group companies are designed for authorised civilian, commercial, and research purposes.

**General Prohibition**

Customers shall not, and shall ensure that its affiliates, end users, and any third parties acting on its behalf do not, use the Products (including SIMs, connectivity, platforms, or any associated infrastructure) in connection with any Prohibited Use as set out in this Statement.

**Military and Defence Use**

Without limitation, the Services shall not be used for:

a) the development, testing, production, operation, maintenance, or support of weapons, munitions, or weapons systems of any kind;
b) military command, control, communications, intelligence, surveillance, or reconnaissance systems ("C4ISR") where such systems are intended for or deployed in active or operational combat environments;
c) the operation, navigation, targeting, or control of unmanned or autonomous vehicles, platforms, or systems that are designed or adapted for the delivery of force or lethal effect; and/or
d) any application directly supporting combat operations or tactical military activities.

**Dual-Use and Government Applications**

Use of the Services in government, security, or dual-use contexts is permitted only where such use is strictly non-combat in nature and does not fall within the scope of prohibited military applications described in this Statement.

Wireless Logic may, without liability and with immediate effect, suspend or terminate the provision of Services where it reasonably believes that the Services are being used in breach of this Statement or continued provision of the Services may expose Wireless Logic to legal, regulatory, or reputational risk.

## 2 Critical Infrastructure

2.1 Where the Customer's use case involves the provision of connectivity to critical national infrastructure (including, without limitation, public transport, utilities or traffic management systems), the Customer must notify Wireless Logic in writing before that use commences.

2.2 The Customer must inform Wireless Logic whether it, or the relevant Customer Entity, is regulated under the UK Network and Information Systems Regulations 2018 (as amended from time to time) or, where applicable, EU Regulation 2022/2555 (NIS2), and must not impose any related cybersecurity, audit or incident-reporting obligations on Wireless Logic except as agreed by Wireless Logic in writing.

2.3 The Customer must not rely on the Products as the sole means of connectivity for any safety-critical or life-critical system without Wireless Logic's prior written agreement as to the applicable service levels.

## 3 Medical Devices

3.1 The Customer must notify Wireless Logic in writing before using the Products in connection with any medical device, including remote patient monitoring, telehealth or clinical alarm systems.

3.2 The Customer must not use the Products as the sole means of connectivity for any device where loss of connectivity could endanger a patient's life or safety, without Wireless Logic's prior written agreement.

3.3 The Customer must provide Wireless Logic with such details of the intended use case as Wireless Logic reasonably requests.

## 4 Drones and Unmanned Aircraft Systems

4.1 The Customer must notify Wireless Logic in writing before using the Products in connection with any drone or unmanned aircraft system ("UAS"), whether operated within visual line of sight ("VLOS") or beyond visual line of sight ("BVLOS").

4.2 Where the use case involves BVLOS operation, the Customer must confirm to Wireless Logic whether it holds, or has applied for, an Ofcom UAS Operator Radio Licence (or the equivalent authorisation in the relevant territory).

4.3 The Customer acknowledges that Wireless Logic does not own the underlying mobile network and that written permission from the relevant Network Provider is required before the Products may be used for airborne connectivity. The Customer must not use, and must not permit any Customer Entity or End User to use, the Products for this purpose until Wireless Logic has confirmed in writing that such permission has been obtained.

4.4 The Customer must ensure that any equipment connected to the Products does not access the 2500–2690MHz (2.6GHz) frequency band while airborne.

## 5 Unmanned Vehicles and Robotics

5.1 The Customer must notify Wireless Logic in writing before using the Products to control the navigation, or any other safety-critical function, of an autonomous or unmanned ground or surface vehicle, or item of robotics.

5.2 The Customer must not use the Products in connection with any vehicle, vessel or system that is weaponised or otherwise adapted for military use (see paragraph 1 above).

## 6 Maritime

6.1 The Customer must notify Wireless Logic in writing before using the Products on board, or in connection with, any vessel.

6.2 The Customer must, on request, provide details of the relevant vessel's ownership and flag state, and must confirm that neither the vessel nor its owner or operator is a Sanctioned Person or otherwise subject to an applicable sanctions regime.

6.3 The Customer must not rely on the Products as the sole means of safety-critical navigation or distress communication (including under the Global Maritime Distress and Safety System) without Wireless Logic's prior written agreement.

## 7 Lone Worker and Personal Safety Devices

7.1 The Customer must notify Wireless Logic in writing before using the Products in connection with any lone worker alarm or personal safety device.

7.2 The Customer must satisfy Wireless Logic that appropriate failover or backup arrangements are in place such that a loss of connectivity does not prevent an emergency call or alert from being raised.

7.3 Where the Customer uses the Products to track the location of any employee or worker, the Customer must comply with Data Protection Legislation and must be able to demonstrate such compliance to Wireless Logic on request.

## 8 Data Centre – Storage of Data

8.1 The Customer must notify Wireless Logic of the location(s) in which any data collected or transmitted using the Products will be stored.

8.2 Where such data is, or may be, transferred outside the United Kingdom or European Economic Area, the Customer must ensure that the safeguards required by Data Protection Legislation are in place, and must enter into a data processing agreement with Wireless Logic where reasonably required by Wireless Logic.

8.3 The Customer must notify Wireless Logic if the relevant data centre or hosted workload involves government or defence tenants or end users.

## 9 Voice-to-Voice Calling and Number-Based Services

9.1 The Customer must comply with the Regulatory Schedule in respect of any use of the Products involving number-based voice services, including in relation to Caller Line Identification and access to emergency organisations.

9.2 The Customer must not use the Products to originate, or knowingly permit the origination of, any call with invalid, altered or spoofed Caller Line Identification.

9.3 The Customer must notify Wireless Logic in advance of its intended use case and expected call volumes for any number-based voice service.

## 10 New Territories and Sanctions

10.1 The Customer must notify Wireless Logic in writing before using, or permitting any Customer Entity or End User to use, the Products in any country or territory not previously notified to, and accepted by, Wireless Logic.

10.2 The Customer warrants that neither it, nor any Customer Entity, End User, or other person on whose behalf it acts, is a Sanctioned Person, or is located, organised or resident in a Sanctioned Territory.

10.3 The Customer must cooperate fully with any sanctions or export control screening reasonably requested by Wireless Logic and must provide such information as Wireless Logic reasonably requires for that purpose.

## 11 Other Use Cases

11.1 This Annex 1 does not describe every use case that may carry additional risk. The Customer must notify Wireless Logic in writing before using the Products for any use case not described above which the Customer knows, or ought reasonably to know, is safety-critical, high-risk, or subject to specific regulatory requirements.

11.2 If the Customer is in any doubt as to whether a use case falls within this Annex 1, the Customer must contact Wireless Logic before proceeding.